MIGLIACCIO & RATHOD LLP
Nicholas Migliaccio (New York Bar No. 4035838)
Jason Rathod (*pro hac vice* anticipated)
Bryan G. Faubus (New York Bar No. 4894101)
412 H St. NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

MATTHEW MARDEN, individually and on behalf of all others similarly situated, Plaintiff, v. LIFEMD, INC., a Delaware corporation, Defendant.	**Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Matthew Marden ("Plaintiff"), individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby alleges the following against Defendant LifeMD, Inc., which conducts business under the brand name Rex MD ("Rex MD" or "Defendant"). Facts pertaining to Plaintiff and his personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon the investigation of counsel and upon information and good faith belief.

NATURE OF THE ACTION

1. This is a class action lawsuit for damages and injunctive relief arising from Rex MD's unlawful practice of disclosing Plaintiff's and Class members' individually identifiable health information ("IIHI") and protected health information ("PHI") (referred to herein collectively as "Private Information") to unauthorized third parties including, but not limited to, Meta Platforms, Inc. d/b/a Meta (referred to herein as "Facebook"), Google LLC, and TikTok Inc. (collectively, the "Pixel Information Recipients").

2. Defendant owns, controls, and maintains the website https://www.RexMD.com/ (referred to herein as the "Website" or "Defendant's Website"), a "telehealth" website that connects patients with doctors who conduct medical assessments and prescribe medications over the internet. Defendant's Website specifically caters to men's health issues, including erectile dysfunction and hair loss. The Website requires individuals to share highly sensitive IIHI and PHI in order to create accounts and to participate in highly sensitive and personal health screenings and receive treatment plans.

3. In order to improve its advertising and thereby increase its profits, Defendant installed and implemented "pixels" and similar tracking technologies such as those made available by the Pixel Information Recipients (referred to herein as the "Pixels") on the Website.

4. Invisible to the naked eye, each of the Pixels collects and transmits information from the user's browser to the corresponding Pixel Information Recipient as the user enters information into the Website. The Pixels secretly enable the unauthorized transmission and disclosure of Plaintiff's and Class Members' IIHI and PHI by Defendant.

5. Defendant also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on the Website. Conversions API serves the same purpose as the Pixels in that it surreptitiously collects and transmits Private Information to Facebook. Unlike the Pixels, however, Conversions API functions from Defendant's servers and therefore cannot be stymied by use of anti-Pixel software or other workarounds. Defendant secretly enabled

additional unauthorized transmissions and disclosures of Plaintiff's and Class members' IIHI and PHI to Facebook by implementing the Conversions API.[1]

6. Through the use of the Pixels and Conversions API, Defendant's Website directs Plaintiff's and Class members' communications to automatically be sent to the servers of the corresponding Pixel Information Recipients. This occurs on every webpage in which Defendant installed the Pixels and for which Defendant enabled Conversions API.[2]

7. Thus, operating as implemented by Defendant, the Pixels and Conversions API allow the Private Information that Plaintiff and Class members submit to them in confidence to be unlawfully disclosed to the Pixel Information Recipients alongside the individual's unique personal identifiers, including his or her Facebook ID and other identifying information pertaining to any accounts they may have with any of the Pixel Information Recipients.

The Tracking Pixel

8. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[3] as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

9. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting—*i.e.*, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

10. Here, a user's web browser executes the Pixels via instructions within each webpage of Defendant's Website to communicate certain information (according to parameters set by Defendant) directly to the corresponding Pixel Information Recipients.

---

[1] "Conversions API works with your Facebook Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited August 4, 2023).

[2] "Server events are linked to a dataset ID and are processed like events sent via the [Facebook] Pixel … This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *See* https://developers.facebook.com/docs/marketing-api/conversions-api (last visited August 4, 2023).

[3] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited August 4, 2023).

11. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[4] stored on their computer by any of the Pixel Information Recipients with which they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser. The Facebook Pixel can access this cookie and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's Website inputs. The same is true for the other Pixel Information Recipients, which also create cookies that are stored in the user's computer and accessed by the Pixels to identify the user.

12. The Pixels are programmable, meaning that Defendant control which of the webpages on the Website contain the Pixels, and which events are tracked and transmitted to the Pixel Information Recipients.

13. Defendant has utilized the Pixels and other tracking technologies since at least January 2017.

14. Defendant used the data they collected from Plaintiff and Class members, without their consent, in an effort to improve their advertising and bolster their revenues.

Conversions API

15. The Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events, and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.[5]

16. Conversions API creates a direct and reliable connection between marketing data (such as a user's private and confidential actions on Defendant's Website) from Defendant's server to Facebook.[6] In doing so, Defendant stores Plaintiff's and Class members' Private Information on their own server and then transmits it to unauthorized third parties.

---

[4] "Cookies are small files of information that a web server generates and sends to a web browser Cookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are- cookies/ (last visited August 4, 2023).

[5] https://revealbot.com/blog/facebook-conversions-api/ (last visited August 4, 2023).

[6] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited August 4, 2023).

17. Conversions API is an alternative method of tracking versus the Facebook Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas the Pixels are "client-side," *i.e.*, executed on users' computers in their web browsers.

18. Because Conversions API is server-side, it cannot access the Facebook-specific cookie to retrieve the user's Facebook ID.[7] Therefore, other roundabout methods of linking the user to their Facebook account are employed by Facebook.[8] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[9]

19. Conversions API tracks the user's website interaction, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

This Lawsuit

20. Plaintiff brings this lawsuit on behalf of similarly situated individuals whose sensitive Private Information was intentionally, recklessly, and/or negligently disclosed to the Pixel Information Recipients through Defendant's unauthorized utilization of the Pixels, Conversions API, and other similar tracking technologies.

21. The Private Information compromised by Defendant's use of the Pixels and related tracking technologies included the Private Information that Plaintiff and Class members submitted to

---

[7] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing- api/conversions-api/parameters/customer-information-parameters/ (last visited August 4, 2023).

[8] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited August 4, 2023).

[9] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited August 4, 2023).

Defendant's Website, including for example, particular health conditions, types of health treatment sought and/or received, age, and other confidential IIHI and PHI.

22. The Pixel Information Recipients in turn use Plaintiff's and Class members' Private Information for business purposes, including using such information to improve advertisers' ability to target specific demographics and selling such information to third-party marketers who target Plaintiff and Class members online (*i.e.*, through their Facebook, Instagram, TikTok, and other social media and personal accounts).

23. Here, Plaintiff and Class members submitted Private Information to Defendant's Website in order to participate in health assessments and other health-related services offered through the Website.

24. Concurrently, this information was communicated from the Website (via the Pixels and Conversions API) to the Pixel Information Recipients: from the Facebook Pixel and Conversions API to Facebook, and from the other Pixels to their respective recipients.

25. In sum, Plaintiff and Class members provided their Private Information to Defendant by creating accounts, completing health assessments, researching doctors and other health-related services providers, making appointments, reviewing conditions and available treatments, researching prescriptions, and/or purchasing subscription plans and, at all times throughout this process, had a reasonable expectation of privacy in the Private Information Defendant were collecting, including that Defendant would ensure that such Private Information remain secure and protected and only utilized for limited medical and health purposes.

26. Defendant further made express and implied promises to protect Plaintiff's and Class members' Private Information and maintain the privacy and confidentiality thereof.

27. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Defendant assumed legal and equitable duties to patients to protect and safeguard their Private Information from unauthorized disclosure.

28. Defendant, however, failed in its obligations and promises by utilizing the Pixels and Conversions API on the Website as described herein, knowing that such technology would transmit and share Plaintiff's and Class members' Private Information with the Pixel Information Recipients.

29. While Defendant willfully and intentionally incorporated the Pixels and Conversions API into the Website, Defendant never disclosed to Plaintiff or Class members that it shared their Private Information, such as their sensitive and confidential assessment responses via the Website, with third parties. As a result, Plaintiff and Class members were unaware that their IIHI and PHI were being surreptitiously transmitted to the Pixel Information Recipients as they participated in health assessments and other health-related activities on Defendant's Website.

30. Despite the stigmas that unfortunately are so often associated with certain health issues and treatments, Defendant intentionally chose to put its profits over the privacy of its users, which number several million. The unilateral disclosure of users' Private Information in this manner is unquestionably a violation of HIPAA, among other statutory and common laws.

31. The disclosure of Plaintiff's and Class Members' Private Information via the Pixels contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information. [10]

32. The HIPAA Privacy Rule sets forth policies to protect all IIHI that is held or transmitted by a covered entity such as Defendant. These are the 18 HIPAA Identifiers that are considered personally identifiable information because this information can be used to identify, contact, or locate a specific person or can be used with other sources (such as a person's Facebook account) to identify a single individual. When IIHI is used in conjunction with one's physical or mental health or condition, health care, and/or one's payment for that health care, it becomes PHI.[11]

---

[10] HHS.gov, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited August 4, 2023).

[11] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited August 4, 2023) (HIPAA Identifiers include name; address (all geographic

33. While healthcare entities regulated under HIPAA may use third-party tracking tools, such as Google Analytics or the Facebook Pixel, they can do so only in a very limited way, to perform analysis on data key to operations.

34. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are simply ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent.

35. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights ("OCR") at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (the "HHS OCR Bulletin"), that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[12]

36. Defendant breached its obligations to Plaintiff and the Class members in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' Private Information; (iii) failing to obtain the consent of patients, including Plaintiff and Class members, to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class members' Private Information through the Pixels and Conversions API; (v) failing to warn Plaintiff and Class

---

subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

[12] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited August 4, 2023).

members of such sharing and disclosures; (vi) otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

37. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the transmissions of their Private Information to the Pixel Information Recipients, (iii) loss of the benefit of the bargain, (iv) diminution of value of the disclosed Private Information, (v) statutory damages, and (vi) the continued and ongoing risk to their Private Information. Plaintiff seeks to remedy these harms and bring causes of action for: (1) negligence; (2) invasion of privacy, (3) breach of confidence; (4) unjust enrichment; (5) violations of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1); (6) violations of the New York General Business Law § 349, N.Y. Gen. Bus. Law § 349 *et seq.*; (7) violations of the New York Information Security Breach and Notification Act, N.Y. Gen. Bus. Law § 899-aa, *et seq.*; (8) violations of the Massachusetts Data Breach Statute, Mass. Gen. Laws § 93H; and (9) violations of the Massachusetts Consumer Protection Act, Mass. Gen. Laws § 93A et seq.

PARTIES

A. Plaintiff Matthew Marden

38. Plaintiff Matthew Marden is a citizen of the state of Massachusetts residing in Marlborough and brings this action in an individual capacity and on behalf of all others similarly situated.

39. On multiple occasions beginning in or around 2016, Plaintiff Marden utilized Defendant's Website on his personal electronic devices to create an account, research his specific medical conditions and treatments for them, search for doctors, find prescription medication, and schedule appointments. In the process of using Defendant's services, Plaintiff Marden was required to disclose highly sensitive IIHI and PHI to Defendant.

40. While Plaintiff Marden was a user of Defendant's services, he never consented to or authorized the use of his Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

41. Plaintiff Marden had an active Facebook account while he used Defendant's services and he accessed Defendant's Website while logged into his Facebook account on the same device. After providing his Private Information to Defendant through the Website, Plaintiff Marden immediately began seeing targeted health ads as he scrolled through his accounts.

B. Defendant

42. Defendant LifeMD, Inc., is a corporation incorporated in Delaware and headquartered in New York, New York.

43. Defendant provides telehealth and other virtual healthcare services to patients across the country. These services include patient-provider audio/video meetings, lab testing, and prescriptions, and involve the solicitation of medical information from patients. As of December 32, 2022, approximately 680,000 customers and patients have used Defendant's services.[13]

44. Rex MD is a brand of Defendant's focusing on men's health that offers access to virtual medical treatment for a variety of men's health needs. Through Rex MD, patients can consult with an affiliated licensed physician and receive prescriptions from partner pharmacies. Although Rex MD initially launched in the erectile dysfunction treatment market, it now offers treatment for a variety of men's health conditions including premature ejaculation, testosterone, and hair loss. As of December 32, 2022, Rex MD has served more than approximately 390,000 customers and patients.[14]

JURISDICTION & VENUE

45. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because Plaintiff and many putative class members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

---

[13] *Form 10-K*, LifeMD, Inc. (Dec. 31, 2022), *available at* https://www.sec.gov/ix?doc=/Archives/edgar/data/948320/000149315223008560/form10-k.htm#bs002 (last visited August 4, 2023).

[14] *Id.*

46. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of the Website in this District, including decisions regarding the privacy of patients' IIHI and PHI and the incorporation of the Pixels, Conversions API, and other tracking technologies.

47. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiff's and Class members' Private Information; Defendant's principal place of business is located in this District; Defendant collects and redistributes Class members' Private Information in this District; and Defendant caused harm to Class members residing in this District.

FACTUAL ALLEGATIONS

48. Defendant installed the Pixels and Conversion API, as well as other tracking technologies, on many (if not all) of the webpages within the Website and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiff's and Class members' Private Information.

49. In order to understand Defendant's unlawful data-sharing practices, it is important to first understand some of the basic web design and tracking tools at issue.

A. Defendant's Method of Transmitting Plaintiff's and Class Members' Private Information via Pixel and Conversions API

50. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as a computer, tablet, or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

51. Every website is hosted by a computer "server" that holds the website's contents. The

entity(ies) in charge of the website exchange communications with users' client devices as their web browsers query the server through the internet.

52. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

a. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court.)

b. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

c. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

53. A patient's HTTP request essentially asks the Defendant's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the participant's screen as they navigate Defendant's Website.

54. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

55. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

56. The Pixels are Source Code doing just that—surreptitiously transmitting a Website user's communications and inputs to the corresponding Pixel Information Recipient much like a traditional wiretap. When individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that displays the webpage visible to the user, along with Source Code (including the Pixels).

57. Thus, Defendant is, in essence, handing its patients a tapped phone and, once the webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications intended only for Defendant and transmits those communications to the corresponding Pixel Information Recipient.

58. Third parties like the Pixel Information Recipients place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the user associated with the information intercepted (in this case, highly sensitive Private Information).

59. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (*i.e.*, their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

60. Defendant also deposits cookies named _fbp, _ga_, and _gid onto Plaintiff's and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiff and Class Members' computing devices by disguising them as first-party cookies. And without any action or authorization, Defendant commands Plaintiff's and Class Members' computing devices to contemporaneously re-direct the Plaintiff's and Class Members' identifiers and the content of their communications to Facebook and Google.

61. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The fbp cookie emanates from Defendant's Website as a putative first-party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. The __ga and _gid cookies operate similarly as to Google.

62. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information.

B. Facebook's Platform & its Business Tools.

63. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[15]

64. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

65. Facebook's Business Tools, including the Facebook Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

66. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[16]

---

[15] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx, INVESTOR.FB.COM (last visited August 4, 2023).

[16] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142, FACEBOOK.COM (last visited August 4, 2023); *see*, META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/, FACEBOOK.COM (last visited August 4, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142, FACEBOOK.COM (last visited August 4, 2023); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/, FACEBOOK. COM (last visited August 4, 2023).

67. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[17]

68. One such Business Tool is the Facebook Pixel, which "tracks the people and type of actions they take" on a webpage in which the Pixel has been installed[18]

69. When a user accesses a webpage that is hosting the Facebook Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent from the user's browser to Facebook's server.

70. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

71. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Website, including not only their medical searches, treatment requests, and the webpages they view, but also their unique personal identifiers including email address and/or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[19] Plaintiff's and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

72. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When the website

---

[17] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK.COM (last visited August 4, 2023); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[18] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK.COM (last visited August 4, 2023

[19] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited June 29, 2023).

visitor is also a Facebook user, the information collected via the Facebook Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, *i.e.*, their real-world identity. Likewise, Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Facebook Pixel to the user's real-world identity using their shadow profile.[20]

73. A user's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

74. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendant and other advertisers and/or sells that information to marketers who will online target Plaintiff and Class members.

75. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that even savvy users cannot evade. Facebook's workaround is called Conversions API. Conversions API is effective because it transmits directly from the host server and does not rely on the user's web browser.

76. Thus, the communications between patients and Defendant, which are necessary to achieve the purpose of Defendant's Website, are received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those

[20] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited August 4, 2023).

communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

77. Although prior to discovery there is no way to confirm that Defendant has implemented Conversions API or another workaround (as that would require accessing the host server), Facebook instructs website owners like Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[21] Thus, it is reasonable to infer that Defendant is utilizing the Conversions API workaround.

78. The Pixel Information Recipients track user data and communications for their own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

79. Thus, without any knowledge, authorization, or action by a user, website owners like Defendant use source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

80. In this case, Defendant employed the Pixels and Conversions API, among other tracking technologies, to intercept, duplicate, and re-direct Plaintiff's and Class members' Private Information to Facebook and the other Pixel Information Recipients.

81. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiff's and Class members' highly sensitive communications and Private Information to the corresponding Pixel Information Recipient, which communications contained private and confidential medical information. These transmissions were performed without Plaintiff's or Class members' knowledge, consent, or express written authorization.

C. Defendant's Use of the Pixels Violated Its Own Privacy Policies

82. Defendant breached Plaintiff's and Class members' right to privacy by unlawfully disclosing their Private Information to the Pixel Information Recipients. Specifically, Plaintiff and Class members had a reasonable expectation of privacy (based on Defendant's own representations

[21] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last access August 4, 2023).

to Plaintiff and the Class that Defendant would not disclose their Private Information to third parties.

83. Specifically, Defendant did not inform Plaintiff that it shared his Private Information with Facebook and the other Pixel Information Recipients. Moreover, Rex MD's Privacy and Personal Information Policy between September 9, 2019, and June 30, 2023 (the "Privacy Policy"), does not explain that user and patient Private Information will be shared with Facebook or other unauthorized third parties. In fact, the Privacy Policy expressly states:

> REX MD . . . automatically receives and records high tech non-personal information on our server logs from your browser including your IP address, cookie information and the page you requested. REX MD may use this information to customize the information, advertising and content you see and to fulfill your requests for certain products and services; with the ultimategoal [*sic*] to ensure your shopping experience is of the highest quality. **You can be assured, REX MD does not connect this non-personal data to any personal information collected from you**.[22]

At best, this assurance is misleading. The Pixels allow the Pixel Information Recipients to link "non-personal data" such as IP addresses and cookie information to personal information entered into Defendant's Website by patients.

84. Furthermore, Defendant's Privacy Policy claims that the information entered into the Website by a patient is "protected for your privacy and security," and that Defendant "safeguard[s] your personal information from unauthorized access, through access control procedures, network firewalls and physical security measures."[23]

85. The Privacy Policy does acknowledge that:

> REX MD may disclose your personal information to sister sites REX MD who workon [*sic*] behalf of REX MD to provide complementary products and services requested by you. **We will share personal information for these purposes only** as our sister sites REX MD [*sic*] have privacy policies that mirror ours or who agree to abide by our collective policies with respect to personal information.[24]

This section continues by listing four circumstances in which "REX MD may otherwise disclose

---

[22] *Rex MD Privacy and Personal Information Policy* (Sep. 9, 2019), *available at* https://rexmd.com/privacy.php (last visited August 4, 2023).

[23] *Id.*

[24] *Id.*

your personal information," including with "express consent to share the information for a specified purpose."[25] None of the four purposes listed circumstances cover Defendant's actions here, i.e., sharing the Private Information of Plaintiff and the Class members with the Pixel Information Recipients for business purposes.

86. Elsewhere in the Privacy Policy, Rex MD acknowledges its use of third-party vendors to conduct remarketing, but it does not disclose that this process involves the wholesale sharing of Plaintiff's and the Class members' Private Information:

> Rex MD has implemented display advertising and uses remarketing with Google analytics to communicate and advertise online. It means that third-party vendors, including Google, show our ads on sites across the Internet to ensure you stay informed of our latest specials and products of interest.
>
> REX MD along with third-party vendors, including Google, use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize, and serve ads based on your past visits to our website. This is typical with your other website browsing activities.[26]

This description of remarketing is misleading, especially in context, alongside the assurances discussed above.

87. By engaging in this improper sharing of information with the Pixel Information Recipients without Plaintiff's and Class members' consent, Defendant violated its own Privacy Policy and breached Plaintiff's and Class members' right to privacy and unlawfully disclosed their Private Information.

88. As a "redundant" measure to ensure Plaintiff's and Class members' Private Information was successfully transmitted to third parties like Facebook, Defendant also implemented server-based workarounds like Conversions API to send Plaintiff's and Class members' Private Information from electronic storage on Defendant's server directly to Facebook, at a minimum.

D. Defendant's Use of the Pixels Violates HIPAA

---

25 *Id.*
26 *Id.*

89. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[27]

90. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

91. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

92. The Privacy Rule broadly defines "protected health information" as individually identifiable health information that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

93. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

94. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods

[27] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

…

H. Medical record numbers;

…

J. Account numbers;

…

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; … and

P. Any other unique identifying number, characteristic, or code… and"

The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

95. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

96. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[28]

---

[28] *See Guidance Regarding Methods for De-Identification of Protected Health Information in*

97. Consistent with this restriction, the HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[29]

98. Here, Defendant provided patient information to third parties in violation of the Privacy Rule. Defendant's Privacy Policy takes the untenable and unsupported position that HIPAA does not apply to a user's basic personal information, stating that "your name, email address, shipping address and phone number . . . we do not consider to be 'protected health information' or 'medical information.'"[30] The Privacy Policy further states "any information that does not constitute Protected Information under applicable laws may be used or disclosed in any manner permitted under this Privacy Policy." As discussed above, this information is clearly protected by the HIPAA Privacy Rule.

99. Rex MD's cavalier attitude towards patient information appears to stem from its mistaken belief that HIPAA does not apply to it. To wit, the Privacy Policy states that "REX MD is not a 'covered entity' under" HIPAA, explaining that "[i]t is important to note that HIPAA does not necessarily apply to an entity or person simply because there is health information involved, and HIPAA may not apply to your transactions or communications with REX MD, the Medical Groups, the Providers or the Pharmacies."[31] Nevertheless, the Privacy Policy also acknowledges that Rex MD "may be subject to certain provisions of HIPAA with respect to "protected health information" provided by patients to affiliated covered entities "[t]o the extent REX MD is deemed a "business

---

Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited August 4, 2023).

[29] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html, HHS.GOV (last visited August 4, 2023).

[30] *Rex MD Privacy and Personal Information Policy* (Sep. 9, 2019), *available at* https://rexmd.com/privacy.php (last visited August 4, 2023).

[31] *Id.*

associate" [of a covered entity], and solely in its role as a business associate."[32]

100. Defendant's equivocation is not a valid legal analysis—ultimately, Rex MD is subject to HIPAA and failed to abide by the HIPAA Privacy Rule in implementing the Pixels and related tracking technologies on its Website.

101. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

102. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation ofc45 C.F.R. section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3);

f. Failing to ensure compliance with HIPAA security standard rules requiring adequate workforce comprehensive training instead of training software used to test staff by imitating phishing emails in violation of 45 C.F.R. section 164.306(a)(4);

[32] *Id.*

g. Failing to effectively train its workforce (including independent contractors) on the policies and procedures for PHI as necessary and appropriate to carry out job functions while maintaining security of PHI beyond using imitation phishing email software in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

h. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

103. Commenting on a June 2022 report discussing the use of Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[33]

104. Defendant's use of third-party tracking code on its Website is a violation of Plaintiff's and Class members' privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA itself, this violation demonstrates Defendant's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

E. Defendant's Use of the Pixels Violates OCR Guidance

105. In addition, the government has issued guidance warning that tracking technologies like the Pixels may come up against federal privacy law when installed on healthcare websites.

106. As mentioned previously, the HHS OCR has issued a bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities And Business Associates* (the "Bulletin"), which provides that healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or the Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[34]

107. According to the Bulletin, Defendant has violated HIPAA rules by implementing the

---

[33] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited August 4, 2023).

[34] *See* HHS OCR Bulletin, *supra* n. 16.

Pixels.[35]

108. The Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[36]

109. Plaintiff and Class members face the same risks warned of above.

110. Defendant has shared Plaintiff's and Class members' IIHI and PHI, including: search terms about health conditions for which they seek doctors; their contacts with doctors to make appointments; the names of their doctors; the frequency with which they take steps to obtain healthcare for certain conditions; and where they seek medical treatment. This information is, as described in the Bulletin, "highly sensitive."

111. The Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[37]

112. Crucially, the government's Bulletin continues:

---

[35] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

[36] *Id.* (emphasis added.)

[37] *Id.* (emphasis added.)

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.***[38]

113. Defendant's sharing of Private Information to the Pixel Information Recipients violated Plaintiff's and Class Members' rights.

F. Defendant Violated Industry Standards.

114. It is a cardinal rule that a medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship.

115. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

116. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.]

117. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be

[38] *Id.* (emphasis added.)

granted.

118. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[39]

119. Defendant's use of the Pixels also violates Federal Trade Commission ("FTC") data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

120. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[40] established cyber-security guidelines for businesses.

121. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

122. Defendant failed to implement these basic, industry-wide data security practices.

G. Users' Reasonable Expectation of Privacy.

123. Plaintiff and Class members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

124. Indeed, at all times when Plaintiff and Class Members provided their IIHI and PHI to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

125. Privacy polls and studies show that the overwhelming majority of Americans

---

[39] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited August 4, 2023).

[40] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 4, 2023).

consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

126. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[41]

127. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class members.

H. IP Addresses are Protected Health Information.

128. Defendant improperly disclosed Plaintiff's and Class Members' computer IP addresses to the Pixel Information Recipients through their use of the Pixels *in addition to* unique personal identifiers such as phone numbers, email addresses, dates of birth, Defendant's client ID numbers, services selected, assessment responses, patient statuses, medical conditions, treatments, provider information, and appointment information.

129. An IP address is a number that identifies the address of a device connected to the Internet.

130. IP addresses are used to identify and route communications on the Internet.

131. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

132. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

133. Facebook, Google, and other third-party marketing companies track IP addresses for targeting individual homes and their occupants with advertising.

134. Under HIPAA, an IP address is considered personally identifiable information,

---

[41] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/, CONSUMERREPORTS.ORG (last visited August 4, 2023).

defining personally identifiable information as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. 45 C.F.R. § 164.514 (2).

135. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

136. Consequently, Defendant's disclosure of Plaintiff's and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

I. Defendant Was Enriched and Benefitted from the Use of the Pixel and other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein

137. The purpose of the use of the Pixels and other tracking technologies on Defendant's Website was to improve marketing and thereby boost revenues.

138. In exchange for disclosing the Private Information of their accountholders and patients, Defendant is compensated by the Pixel Information Recipients in the form of enhanced advertising services and more cost-efficient marketing on their platform.

139. Defendant was advertising their services through Facebook, for one, and the Pixels were used to "help [Defendant] understand which types of ads and platforms are getting the most engagement[.]"[42]

140. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions.

141. Defendant retargeted patients and potential patients to get more people to use their services. These patients include Plaintiff and Class members.

142. Thus, utilizing the Pixels benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

143. Moreover, Plaintiff's and Class members' Private Information had value and

---

[42] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited August 4, 2023).

Defendant's disclosure and interception harmed Plaintiff and the Class.

144. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to increase: estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

145. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[43]

146. Similarly, CNBC published an article in 2019 in which it observed that "[p]atient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[44]

147. Tech companies are under particular scrutiny because they already have access to massive troves of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

148. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[45]

149. Private Information is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[46] A robust "cyber black market" exists where criminals openly post stolen IIHI and PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

43 *See* https://time.com/4588104/medical-data-industry/ (last visited August 4, 2023).

44 *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited August 4, 2023).

45 *Id.*

46 Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited August 4, 2023).

150. While credit card information and associated IIHI can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363.[47]

151. PHI is particularly valuable because criminals can use it to target victims with frauds that take advantage of their medical conditions.

152. PHI can also be used to create fraudulent insurance claims, facilitate the purchase and resale of medical equipment, and help criminals gain access to prescriptions for illegal use or sale.

153. Medical identity theft can result in inaccuracies in medical records, costly false claims, and life-threatening consequences. If a victim's health information is commingled with other records, it can lead to misdiagnoses or mistreatment.

154. The FBI Cyber Division issued a Private Industry Notification on April 8, 2014, that advised the following:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

155. Cybercriminals often trade stolen Private Information on the black market for years following a breach or disclosure. Stolen Private Information can be posted on the Internet, making it publicly available.

156. Defendant gave away Plaintiff's and Class Members' Private Information without permission.

157. The unauthorized access to Plaintiff's and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Website users, including Plaintiff and Class Members.

158. Plaintiff suffered damages in the form of (a) invasion of privacy; (b) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (c) diminution of value of the Private Information; (d) statutory damages; (e) the continued

---

[47] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited August 4, 2023).

and ongoing risk to his Private Information; (f) lost benefit of the bargain; and (g) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information he communicated to Defendant via the Website.

159. Plaintiff have a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

TOLLING

160. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know—and had no way of knowing—that his Private Information was intercepted and unlawfully disclosed to the Pixel Information Recipients because Defendant kept this information secret.

CLASS ALLEGATIONS

161. This action is brought by the named Plaintiff on his behalf and on behalf of a proposed Class of all other persons similarly situated under Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

162. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Pixels and other tracking technologies on Defendant's Website.

163. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff assert claims on behalf of a separate Massachusetts Subclass, which is defined as follows:

> All persons residing in the state of Massachusetts whose Private Information was disclosed to a third party without authorization or consent through the Pixels and other tracking technologies on Defendant's Website.

164. Excluded from the proposed Class and the Subclass are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

165. Plaintiff reserves the right to amend the definitions of the Class and the Subclass or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

166. Numerosity. The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1 million patients that have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

167. Commonality. Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class members. These common questions include, but are not limited to, the following:

a) Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class members;

b) Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class members to unauthorized third parties;

c) Whether Defendant violated its own privacy policy by disclosing the Private Information of Plaintiff and Class members to the Pixel Information Recipients;

d) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their Private Information would be disclosed to third parties;

e) Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their Private Information was being disclosed without their consent;

f) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' Private Information;

g) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Private Information belonging to Plaintiff and Class members free from unauthorized disclosure;

h) Whether Defendant violated the statutes asserted as claims in this Complaint;

i) Whether Plaintiff and Class members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j) Whether Defendant knowingly made false representations as to their data security and/or privacy policy practices;

k) Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices; and

l) Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Private Information.

168. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's Private Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Pixels and/or Conversions API.

169. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

170. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members in that all the Plaintiff's and Class members' data was unlawfully disclosed to unauthorized third parties, including the Pixel Information Recipients, in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

171. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class

members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

172. Defendant has acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

173. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information and not disclosing it to unauthorized third parties;

b) Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c) Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendant adequately and accurately informed Plaintiff and Class members that their Private Information would be disclosed to third parties;

e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

174. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the unauthorized disclosures that have taken place. Class members have already been preliminarily identified and sent Notice by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On behalf of Plaintiff & the Nationwide Class*)

175. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

176. Upon soliciting, accepting, storing, and controlling the Private Information of Plaintiff and the Class, Defendant owed, and continue to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

177. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information from unauthorized disclosure.

178. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information through their use of the Pixels, Conversions API, and other tracking technologies would result in unauthorized third parties, such as the Pixel Information Recipients, gaining access to such Private Information for no lawful purpose.

179. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class members' Private Information arose due to the special relationship that existed between Defendant and their patients, which is recognized by statute, regulations, and the common law.

180. In addition, Defendant had a duty under Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

181. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included the failure to (1)

secure Plaintiff's and Class members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API, and other tracking technologies.

182. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

183. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

184. Plaintiff and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT II
INVASION OF PRIVACY
(*On behalf of Plaintiff & the Nationwide Class*)

185. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

186. The highly sensitive and personal Private Information of Plaintiff and Class members consists of private and confidential facts and information regarding Plaintiff's and Class members' health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

187. Plaintiff and Class members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including the Pixel Information Recipients.

188. Defendant owed a duty to Plaintiff and Class members to keep their Private Information confidential.

189. Defendant's unauthorized disclosure of Plaintiff's and Class members' Private Information to the Pixel Information Recipients—third-party tech and marketing giants who use such information for their own business purposes—is highly offensive to a reasonable person.

190. Defendant's willful and intentional disclosure of Plaintiff's and Class members' Private Information constitutes an intentional interference with Plaintiff's and Class members' interest in solitude and/or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

191. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class members' privacy because Defendant facilitated the Pixel Information Recipients' simultaneous eavesdropping and wiretapping of confidential communications.

192. Defendant failed to protect Plaintiff's and Class members' Private Information and acted knowingly when they installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate individual's communications on the Website for the purpose of marketing and advertising.

193. Because Defendant intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Defendant had notice and knew that their practices would cause injury to Plaintiff and the Class.

194. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information, including the IIHI and PHI of Plaintiff and Class members, was disclosed to unauthorized third parties, causing Plaintiff and the Class to suffer damages.

195. Plaintiff, on behalf of himself and Class members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, lost benefit of the bargain, plus pre-judgment interest and costs.

196. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the

possession of the Pixel Information Recipients, and the wrongful disclosure of the Private Information cannot be undone.

197. Plaintiff and Class members have no adequate remedy at law for the injuries relating to Defendant's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendant's disclosure of the Private Information to unauthorized third parties who continue to possess and utilize the Private Information.

198. Plaintiff, on behalf of himself and Class members, further seeks injunctive relief to enjoin Defendant from intruding into the privacy and confidentiality of Plaintiff's and Class members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
BREACH OF CONFIDENCE
(*On behalf of Plaintiff & the Nationwide Class*)

199. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

200. Possessors of non-public medical information, such as Defendant, have a duty to keep such medical information completely confidential.

201. Plaintiff and Class members had reasonable expectations of privacy in the responses and communications entrusted to Defendant through their Website, which included highly sensitive Private Information.

202. Contrary to its duties as a telehealth services provider and its express promises of confidentiality, Defendant installed the Pixels and Conversions API to disclose and transmit to third parties Plaintiff's and Class members' Private Information, including data relating to Plaintiff's and Class members' health.

203. These disclosures were made without Plaintiff's or Class members' knowledge, consent, or authorization.

204. The third-party recipients included, but may not be limited to, the Pixel Information Recipients.

205. As a direct and proximate cause of Defendant's unauthorized disclosures of Plaintiff's and Class members' Private Information, Plaintiff and Class members were damaged by Defendant's breach of confidentiality in that (a) sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private; (b) Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) Defendant eroded the essential confidential nature of health services that Plaintiff and Class members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiff and Class members and the obtaining of a benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensation to Plaintiff or Class members for the unauthorized use of such data; (g) diminishment of the value of Plaintiff's and Class members' Private Information; and (h) violation of property rights Plaintiff and Class members have in their Private Information.

COUNT IV
UNJUST ENRICHMENT
(*On behalf of Plaintiff & the Nationwide Class*)

206. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

207. Defendant has benefitted from the use of Plaintiff's and Class members' Private Information and unjustly retained those benefits at Plaintiff's and Class members' expense.

208. Plaintiff and Class members conferred a benefit upon Defendant in the form of the monetizable Private Information that Defendant collected from them and disclosed to third parties, including the Pixel Information Recipients, without authorization and proper compensation.

209. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

210. Defendant unjustly retained those benefits at the expense of Plaintiff and Class members because Defendant's conduct damaged Plaintiff and Class members, all without providing any commensurate compensation to Plaintiff or Class members.

211. The benefits that Defendant derived from Plaintiff and Class members were not offered by Plaintiff or Class members gratuitously and, thus, rightly belongs to Plaintiff and Class members. It would be inequitable under unjust enrichment principles in Massachusetts and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

212. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq.*
(*On behalf of Plaintiff & the Nationwide Class*)

213. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

214. The ECPA protects both sent and received communications.

215. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

216. The transmissions of Plaintiff's and Class members' Private Information to Defendant via Defendant's Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

217. The transmission of Private Information between Plaintiff and Class members and Defendant via their Website are "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

218. The ECPA defines "content" when used with respect to electronic communications to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

219. The ECPA defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

220. The ECPA defines "electronic, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class members' browsers;

b. Plaintiff's and Class members' computing devices;

c. Defendant's web-servers; and

d. The Pixels deployed by Defendant to effectuate the sending and acquisition of user and patient sensitive communications.

221. By utilizing and embedding the Pixels and Conversions API on their Website and/or servers, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class members, in violation of 18 U.S.C. § 2511(1)(a).

222. Specifically, Defendant intercepted Plaintiff's and Class members' electronic communications via the Pixels and Conversions API, which tracked, stored, and unlawfully disclosed Plaintiff's and Class members' Private Information to Facebook.

223. Defendant's intercepted communications that included, but are not limited to, communications to/from Plaintiff and Class members regarding IIHI and PHI, including IP address, Facebook ID, and health information relevant to the screenings and treatment plans in which Plaintiff and Class members participated.

224. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class members to the Pixel Information Recipients and, potentially, other third

parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

225. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class members, while knowing or having reason to know that the Information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

226. Defendant intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

227. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixels and Conversions API to track and utilize Plaintiff's and Class members' Private Information for its own financial benefit.

228. Defendant was not acting under color of law to intercept Plaintiff's and Class members' wire or electronic communications.

229. Plaintiff and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class members' privacy via the Pixels and Conversions API.

230. Any purported consent that Defendant received from Plaintiff and Class members was not valid.

231. In sending and in acquiring the content of Plaintiff's and Class members' communications relating to the browsing of Defendant's Website, creation of accounts, participation in Defendant's health screenings, and/or purchasing a subscription plan, Defendant's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

COUNT VI

VIOLATIONS OF THE NEW YORK INFORMATION SECURITY BREACH AND NOTIFICATION ACT
N.Y. Gen. Bus. Law § 899-aa, et seq.
(*On behalf of Plaintiff & the Nationwide Class*)

232. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

233. The acts and practices alleged herein occurred in trade or commerce in the state of New York.

234. Defendant's use of the Pixels and related tracking technologies on its Website, which compromised the Private Information of New York citizens, constitutes a "breach of security," as that term is defined by NY Gen. Stat. §899-aa. 206.

235. In the manner described herein, Defendant unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of NY Gen. Stat. § 899-aa. In fact, Defendant has not yet publicly acknowledged the breach of security caused by its implementation and use of the Pixels.

236. Pursuant to NY Gen. Stat. § 899-aa, Defendant's failure to disclose the unauthorized transmission of Private Information following discovery to each New York resident whose Private Information was, or was reasonably believed to have been, accessed by an unauthorized person through the Breach constitutes an unfair trade practice pursuant to NY. Gen. Stat. § 899-aa.

COUNT VII
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
N.Y. Gen. Bus. Law § 349 et seq (2019)
(*On behalf of Plaintiff & the Nationwide Class*)

237. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

238. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

239. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

240. Defendant solicited Plaintiff's and Class members' Private Information through the Website. Defendant knew or should have known that the use of the Pixels and the related technologies complained of herein did not comply with all relevant regulations and failed to keep Plaintiff's and Class members' Private Information secure and prevent the transmission of that Private Information to unauthorized third parties. Defendant did not disclose to Plaintiff and Class members that it shared their Private Information with the Pixel Information Recipients

241. Plaintiff and Class members would not have provided their Private Information if they had been told or knew that Defendant failed to maintain sufficient security thereof, and in fact shared Plaintiff's and Class members' Private Information for its own business purposes.

242. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information from unauthorized disclosure;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTCA"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data, and HIPAA. Defendant's failure was a direct and proximate cause of the unauthorized disclosure of Plaintiff's and Class members' Private Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information from unauthorized disclosure;

e. Omitting, suppressing, and concealing the material fact that it did not intend to protect Plaintiff's and Class members' Private Information from unauthorized disclosure; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTCA and HIPAA, which failure was a direct and proximate cause of the unauthorized disclosure..

243. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

244. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

245. In addition, Defendant's failure to secure patients' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

246. Defendant knew or should have known that its use of the Pixels and related tracking technologies failed to safeguard the PII of Plaintiff and Class members and in fact ensured that their Private Information would be shared without their knowledge or consent. Plaintiff and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

247. The aforesaid conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

248. Defendant's violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have submitted their Private Information through the Website, and many of those have had their Private

Information shared with the Pixel Information Recipients. In addition, New York residents have a strong interest in regulating the conduct of its retirement and investment services administrators, whose policies described herein have affected thousands of people across the country.

249. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

250. Defendant oversaw its Website and the implementation and use of the Pixels and related tracking technologies complained of herein from New York, and its communications to its patients and the Pixel Information Recipients largely emanated from New York.

251. Most, if not all, of the alleged misrepresentations and omissions by Defendant that led patients to submit Private Information through the Website occurred within or were approved within New York.

252. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

253. Accordingly, Plaintiff, on behalf of himself and Class members, bring this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT IX
VIOLATIONS OF THE MASSACHUSETTS DATA BREACH STATUTE
Mass. Gen. Laws Ch. 93h
(On behalf of Plaintiff & the Massachusetts Subclass)

254. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

255. The acts and practices alleged herein occurred in trade or commerce in the commonwealth of Massachusetts.

256. Defendant's use of the Pixels and related tracking technologies on its Website, which compromised the Private Information of Plaintiff, both Massachusetts citizens, constitutes a "breach of security," as that term is defined by Mass. Gen. Laws ch. 93H, § 3.

257. Defendant has not yet notified Plaintiff or any other member of the Massachusetts Subclass that their Private Information was acquired and used by an unauthorized person or used for an unauthorized purpose.

258. Thus, Defendant has unreasonably delayed the disclosure of the "breach of security" of Private Information within the meaning of Mass. Gen. Laws ch. 93H, § 3.

259. Pursuant to Mass. Laws ch. 93H, Defendant's failure to disclose the unauthorized transmission of Private Information following discovery "as soon as practicable and without unreasonable delays" was a breach of Gen. L. ch. 93H, § 3(b).

COUNT X
VIOLATIONS OF THE MASSACHUSETTS CONSUMER PROTECTION ACT
Mass. Gen. Law § 93a, *et seq.*
(*On behalf of Plaintiff & the Massachusetts Subclass*)

260. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

261. Mass. Gen. Laws ch. 93A et seq. prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Massachusetts.

262. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of G.L.c. 93A. Defendant's conduct alleged herein is a "business practice" within the meaning of G.L.c. 93A, and the deception occurred within the commonwealth of Massachusetts.

263. Plaintiff and other members of the Massachusetts Subclass used Defendant's Website from Massachusetts. Their Private Information was collected and transmitted by operation of the Pixels, which was instantiated in the Source Code running in their browser or mobile application.

264. Defendant solicited, obtained, and stored Plaintiff's and Class members' Private Information and knew or should have known not to disclose such Private Information to the Pixel Information Recipients through use of the Pixels and other tracking technologies.

265. Plaintiff and Class members would not have provided their Private Information if they had been told or knew that Defendant would be disclosing such information to the Pixel Information Recipients and others.

266. As alleged herein, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of Mass. Gen. Laws ch. 93A, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information from unauthorized disclosure;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data, and HIPAA. Defendant's failure was a direct and proximate cause of the unauthorized disclosure of Plaintiff's and Class members' Private Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information from unauthorized disclosure;

e. Omitting, suppressing, and concealing the material fact that it did not intend to protect Plaintiff's and Class members' Private Information from unauthorized disclosure; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Personal Information, including duties imposed by the FTCA and HIPAA, which failure was a direct and proximate cause of the unauthorized disclosure.

267. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

268. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer by providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in Massachusetts through deceptive means were consumer-oriented acts and thereby falls under the Massachusetts consumer protection statute.

269. In addition, Defendant's failure to secure patients' Private Information violated the FTCA and therefore violated the Massachusetts Consumer Protection Act.

270. Defendant knew or should have known that its computer systems and data security practices—in particular, their use of the Pixels and Conversions API—were inadequate to safeguard the IIHI of Plaintiff and Class members, and that enabling third parties to collect the Private Information of Plaintiff and the Massachusetts Subclass constituted a data breach. Plaintiff and Class members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

271. Defendant's violations of the Massachusetts Consumer Protection Act have an impact and general importance to the public, including the people of this commonwealth. Thousands of Massachusetts citizens have had their Private Information transmitted without consent from Defendant's Website to third parties.

272. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class members are entitled to judgment under the Massachusetts Consumer Protection Act, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

273. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of the Massachusetts Consumer Protection Act.

274. Accordingly, Plaintiff, on behalf of himself and Class members, bring this action under Mass. Gen. Laws ch. 93A to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully request that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Nationwide Class and Massachusetts Subclass defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiff's and Class members' Private Information;

c) For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

d) For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded; and

g) Such other and further relief as this court may deem just and proper.

Dated: August 23, 2023

Respectfully submitted,

MIGLIACCIO & RATHOD, LLP

*/s/*_____
Nicholas A. Migliaccio
(New York Bar No. 4035838)
Jason S. Rathod*

Bryan G. Faubus
(New York Bar No. 4894101)
Tel: 202.470.3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

*pro hac vice anticipated

Attorneys for Plaintiff & the Putative Class